System Rules of Behavior

National Aeronautics & Space Administration

Goddard Space Flight Center

System Rules of Behavior for the Sciences and Exploration Directorate (SED) Multi-Program/Project (MPP) IT Science Systems

CD-014-L-GSF-6004

Issue Date: 05-31-2007
Effective Date: 05-31-2007

Verify that this is the correct version before use.

National Aeronautics and
Space Administration

THIS PAGE LEFT INTENTIONALLY BLANK

REVIEW AND APPROVAL SIGNATURE

The SED MPP IT Science Systems Rules of Behavior were prepared for the exclusive use of NASA. I have reviewed and concur with the attached Rules of Behavior.

Approved by: ______________________ 3/2/2007

System Owner Date

DOCUMENT RELEASE VERSION 1.0

REVIEW AND APPROVAL SIGNATURE

The SED MPP IT Science Systems Rules of Behavior were prepared for the exclusive use of NASA. I have reviewed and concur with the attached Rules of Behavior.

Approved by: ______________________ 4/20/07
System Owner Date

DOCUMENT CHANGE HISTORY

Version Number	Date	Author	Description
1.0	7/31/07	Jeff Simpson / Code 600 Directorate Computer Security Engineer (DCSE)	Initial release

Sciences and Exploration Directorate (SED) Multi-Program/Project (MPP) IT Science Systems Rules of Behavior

1.0 INTRODUCTION

The rules of behavior contained in this document are to be followed by all users of the SED MPP IT Science Systems. The rules clearly delineate responsibilities of and expectations for all individuals with access to the system. Users are held accountable for their actions on the SED MPP IT Science Systems. If an employee violates NASA policy regarding the rules of the system, they may be subject to disciplinary action at the discretion of management. Actions may range from a verbal or written warning, removal of system access for a specific period of time, reassignment to other duties, or termination, depending on the severity of the violation.

2.0 RESPONSIBILITIES

The Chief of Information Systems Security is responsible for ensuring that an adequate level of protection is afforded to the SED MPP IT Science Systems through an appropriate mix of technical, administrative, and managerial controls. The Chief develops policies and procedures, ensures the development and presentation of user and contractor awareness sessions, and inspects and spot-checks to determine that an adequate level of compliance with security requirements exists. The Chief is responsible for conducting periodic vulnerability analyses to determine if security controls are adequate. Special attention is given to those new and developing technologies, systems, and applications that can open or have opened vulnerabilities in NASA's security posture.

3.0 OTHER POLICIES AND PROCEDURES

The rules are not to be used in place of existing policy, rather they are intended to enhance and further define the specific rules each user must follow while accessing SED MPP IT Science Systems.

4.0 APPLICATION RULES

Account and Access Control Management: To obtain an account on any NASA multi-user (server) computer, users must first complete an account request form and then obtain signed approval by an authorized government official. Foreign nationals must also submit a National Agency Check (NAC) application either through their Division Office staff, line manager or CSO. Foreign national account request forms must also be approved and signed by the Center IT Security Manager (C-ITSM). Contact the computers system administrator or the organizations Computer Security Official (CSO) for the account request form and guidance on the appropriate authorized government official.

Users must only use accounts for which they are authorized and must not share their account with any other user. Users are responsible for protecting and maintaining to the best of their ability any information that is used or stored in or from their account. Users must not attempt to access any data or program contained on any system for which they are not authorized.

When a users job status or assignment changes such that they no longer require an account, the user must notify either the computers system administrator, the organizations

CSO or the authorized government official and then make no further attempt to access their account.

Anti-virus and Anti-spyware Software: All NASA-owned, contractor-owned or personally-owned Microsoft Windows and Apple Macintosh workstation and laptop computers connected to a NASA network are required to have anti-virus scanning software installed. Users are required to keep the scanning software current with the latest updates and to scan their computers on a frequent basis. GSFC has purchased a site license from McAfee for its anti-virus software for both computer platforms which are available for download at http://cne.gsfc.nasa.gov/application/cne_sppt_sw/index.html#anti. GSFC has also purchased a site license for an anti-spyware scanner product for Microsoft Windows computers called SpySweeper which is available for download from http://gsfc-thor.gsfc.nasa.gov. Consult your system administrator for proper configuration of these products.

Annual IT Security Training: Users must complete the required annual Basic IT Security Awareness Training, or IT Security Awareness Training for Managers if applicable, which are available online at https://satern.nasa.gov. Users are encouraged to print and keep an electronic or hard copy of their training completion certificate. Announcements will be issued indicating the due date for completion. In addition, users are encouraged to browse Satern's online catalog for other course topics that may be applicable to the user's job duties or of general interest. There is no cost to take any of these online courses and they may be taken at any time.

Assignment and Limitation of Privileged System Accounts: *The SED limits access to privileged system accounts (e.g. root, administrator) to system administrators and to a very few trusted technical leaders (scientists or programmers) who demonstrate both a need for this privilege and an understanding of the responsibility that goes along with it. Non-system administrators who share privileged accounts with system administrators agree to guidelines such as notifying the system administrator if any changes are made to the computer's configuration that could potentially affect its security controls. Failure to do so could result in the loss of this privileged access.*

For project computers (servers, lab workstations), system privileges are limited to system administrators and the project technical leader. For individual workstations, system privileges are limited to system administrators and the workstation owner.

Authorized Use of Government IT Resources: Government IT resources (e.g. computer equipment, printers/copiers, networks, etc.) and electronic communication facilities (e.g. email) are for official and authorized Government use only. Users must not use Government IT resources to maintain or operate a personal business or charitable organization, advertise goods or services for sale, engage in any activity for monetary or personal gain, perform consulting work other than that required by the user's job at NASA. Users must consent to monitoring and abide by all applicable acceptable user requirements both in policy (e.g. NPD 2540.1F available at http://itsecurity.nasa.gov/policies/npd_npr/index.html) and as described in the Information Technology (IT) Security 101 Handbook available at http://eitsb.gsfc.nasa.gov/Documents/ITSHandbook_final.pdf. Consult the CSO for guidance on acceptable use policy.

Users must not participate in any activity or information exchange that would violate federal law, regulation or policy. Examples of such activity or information exchange include the creation, downloading, viewing, storing, copying or transmission of material related to illegal weapons, illegal gambling, terrorist activities, child pornography, sexual harassment, hate literature, sexually explicit or sexually oriented material, and racist literature.

Users must not download or install software onto a Government computer that is not applicable to the users job duties and not included as a component of the computer's operating system distribution media (e.g. freeware or shareware games, music or video players). Non-commercial products frequently contain hidden spyware that can track a user's computer use, monitor keyboard activity including typed passwords or even steal copies of sensitive electronic files.

Users are permitted some occasional personal use of electronic mail or the Internet, provided it does not interfere with the employee's work or the work of others. Use of government computing systems for personal use must be limited to brief periods, should not incur any additional expense to the Government, and must not interfere with the user's job duties. When communication cannot reasonably be made during non- business hours, users may exchange brief messages with persons or entities such as a spouse or dependent, someone responsible for the care of a spouse or dependent, state and local government agencies on personal matters, or medical care providers.

Backups: Users must ensure that there are appropriate procedures in place to backup their electronic NASA data. Users are advised to consult with their system administrator to determine whether backups of their system are being performed for them as well as the frequency. Backups of desktop workstations may be left to the responsibility of the user.

Computer Security Patches: Users who perform their own system administration of their computer workstations are responsible for ensuring their workstation are kept as current as possible with all critical operating system patches. Users are strongly encouraged to configure their workstation computers to check for and then download and install operating system patches automatically and that this be performed at least weekly. Users are also responsible for ensuring that Patchlink is installed on their workstation computers. Consult your system administrator or CSO for guidance.

Connecting Computers to the Network: Users must not connect any computer to any NASA wired or wireless network, excluding a guest wireless network, without having first obtained an authorized ip address issued by their CSO. All computers newly connected to the network must also have been scanned for vulnerabilities and have anti-virus and anti-spyware software installed if one exists for the computers operating system type. Computers must also have Patchlink installed if it is available for the computers operating system type. Consult the CSO for guidance.

Connecting Personally Owned Computers: While permissible, use of personally owned computers to connect to any NASA/GSFC network, excluding a guest wireless network, is discouraged. Users must obtain written permission from their line manager or other authorized government official and then abide by all procedures and controls from NPR 2810.1A pertaining to personally-owned IT resources. Consult the CSO for guidance. Users must also accept that if their personally owned computer is involved in an IT security compromise while connected to the GSFC network, the compromise may be considered a crime and the computer may be confiscated and held by law enforcement representatives to collect and preserve evidence.

Consequences of Behavior Inconsistent with these Rules: Failure to abide by these rules may result in administrative action or termination of access privileges. Failure to abide by the rules described in the Handling of Sensitive Information can be more severe.

Dial-In and VPN Access: Dial-in and VPN access is available for all badged civil servant and contractor employees who are registered in GSFC's LISTS (x500) database. This service allows users to remotely access IT resources on the GSFC CNE network from home or while on travel. The account request form and conditions for use are available at http://cne.gsfc.nasa.gov/network/remote_access/Remote_Access_CNE_Network.html.

Email: Users must use their NASA email address (e.g. @nasa.gov or @gsfc.nasa.gov) for official use only as it is a representation of the Agency, analogous to the use of NASA letterhead, in which the opinions expressed reflect on NASA.

Users must use caution and not open any unsolicited or suspicious email, particularly if it contains an attachment, without first verifying its source.

User must not send or forward chain letters, personal mass mailings, hoaxes, or harassing messages.

Handling of Sensitive Information: Users are responsible for determining the level of sensitivity of any non-public scientific, engineering, financial, proprietary or business-sensitive data, either in electronic or hard copy that is in their possession and control. Users must refer to NPR 1600.1 section 5.24 labeled Sensitive But Unclassified (SBU) Controlled Informationfor guidance on what data is considered SBU and how it must be properly marked, handled and stored. The NPR 1600.1 is available online at http://nodis3.gsfc.nasa.gov/lib_docs.cfm?range=1600. Users must also consult with GSFCs export control office for additional guidance on proper handling procedures if the data might be considered International Traffic in Arms Regulations (ITAR) or Export Administrative Regulations (EAR). Improper handling of ITAR or EAR data can result in severe financial or criminal penalties to the user.

In addition to the handling and storage requirements specified by NPR 1600.1, the SED requires that all users maintain all electronic copies of SBU data in encrypted form when stored on disk or other electronic storage media or when transmitted electronically. These files must reside on a computer that has a host-based firewall or packet filtering software enabled to protect against unauthorized access. This computer must also utilize strict file system permissions to restrict read/write access to only those authorized. Users are encouraged to use Entrust PKI for this purpose but can use other forms of encryption such as PGP, Mac OS-X File Vault, or Microsoft Windows Encrypted File System. Users can obtain an Entrust PKI request form from http://cne.gsfc.nasa.gov/security/pki.html. Consult your system administrator or CSO for guidance for other encryption options.

Limits on Workstation Interconnection: Users are discouraged from configuring their workstation computers or laptops to enable login services such as ftp or ssh that allow remote users to access their computer unless the computer is maintained and monitored by a system administrator and the computer meets all security controls specified by NPR 2810.1A.

Moving or Disposal of IT Resources: Users are required to notify their property custodian of any computer that is moved between offices, assigned to another user or is to be excessed. Users are responsible for ensuring that all sensitive information are deleted from the computers hard disk or other storage media prior to it being assigned to another user or to being transferred to excess.

Password Management:

Users must abide by the password requirements from NPR 2810.1A which include changing passwords at least annually, being between 8 and 128 characters in length, containing at least one special character if supported by the operating system, containing at least one character from each of the other three character sets (lower case letter, upper case letter and numerals). Users must choose passwords that are difficult to guess and which are not representative of their name, a family members name, a name or acronym of a NASA organization, or a dictionary word (English or other language) even with numerals used to replace letters.

Users are strongly encouraged to use a different password on each computer for which they have an account. Users should avoid using the same password(s) on any off-site computer not owned and managed by either NASA or a NASA contractor especially if the computer is ever used to remotely log into their account on any NASA/GSFC owned computer.

Users must not write down their password(s) unless then kept locked in a file cabinet, desk drawer or other locked compartment. Users must not store their password(s) in an electronic file unless the file is maintained in an encrypted form (e.g. Entrust PKI, PGP).

Users are forbidden from sharing or divulging their account password(s) to anyone else under any circumstances.

Physical Security: Users must activate their computer's screen lock or log off their computer when left unattended. As applicable, users should also lock their offices when they leave for an extended period.

If an unknown person is observed within their work area and who is not displaying an appropriate badge, users are expected to either ask for proper identification or to contact GSFCs security office.

Proper Use of Copyrighted Software or Information: Users are responsible for ensuring the valid licensing of all software on their workstation computers. Users must not make or use unauthorized copies of copyrighted software or other electronic information except as permitted by law or by the owner of the copyright.

Reporting IT Security Incidents: Users are required to report all observed compromises of IT security (viruses, unauthorized access, theft, inappropriate use, etc.) involving their computer system as soon as possible but no later than within 2 hours of detection. The organizational CSO and system administrator should be contacted first. The list of CSOs along with their contact information is available at http://eitsb.gsfc.nasa.gov/csoListing.html which is organized by Directorate. Call or visit them, do not send clear text email. The CSO and system administrator must then inform the DCSO and their management . If the CSO and system administrator are not immediately available, the user must then contact the DCSO. The list of DCSOs and their contact information is also available at the above URL. If the DCSO is also not immediately available, the user must then contact the Center Information Technology Security Manager (C-ITSM). The list of ITSMs along with their contact information is available at http://eitsb.gsfc.nasa.gov/reps_manager.html.

The user must not continue to use the affected computer or change its operating state (e.g. power off the computer) until they have received instruction from either their system administrator, CSO or C-ITSM.

If the observed compromise involves unauthorized access or theft of a computer containing Personally Identifiable Information (PII), the user must follow the above procedure but also ensure the C-ITSM is contacted no later than 1 hour after detection.

Work At Home: Users working from home must adhere to GSFCs Teleworking Policy (http://ohcm.gsfc.nasa.gov/family/telecommute)which includes first getting approval from your supervisor. If any government-owned computer equipment will be brought home, users must obtain a property pass from their property custodian. If the computer will remain at home for an extended period (1 month or greater), users must consult with their organization's system administration staff prior to first taking the computer equipment home to ensure it is configured to comply with NASA's computer security requirements. Users must then consult with their system administration staff at least monthly to determine whether any new IT security threats exist that may require some specific corrective action. The following rules from this document apply to the use of government-owned computers at home: Dial-in Access, Password Management, Authorized User of Government Equipment, Proper Use of Copyrighted Material, Anti-Virus and Anti-Spyware Software, Reporting IT Security Incidents, Handling of Sensitive Information, Backup Procedures, Restoration of Service, Computer Security Patches, and Basic IT Security Awareness Training. Users must only use this equipment for government-related business and must not allow other family members to access this equipment. Users who fail to abide by these rules will be subject to losing their work at home privileges.

Users working from home should refrain from using a personally-owned computer to process or store non-public NASA data and must **never** do so if the data is identified as being Sensitive But Unclassified (SBU) as defined in NPR 1600.1 section 5.24. If a personally-owned computer is used to process or store non-sensitive NASA data, the user must ensure the computer remains up-to-date with all critical operating system patches as well as anti-virus and anti-spyware updates. It is acceptable to use a personally-owned computer to read email from their NASA/GSFC email account. Users should use discretion or refrain from remotely logging into their account on any NASA/GSFC computer on any NASA/GSFC network either directly via Secure Shell (SSH) or indirectly via the VPN from a personally owned computer or any other computer not owned and managed by either NASA or a NASA contractor. Use of two-factor authentication such as RSA SecurID is highly encouraged in such situations. Consult with the CSO for guidance and to determine available options.

5.0 LETTER FOR EXTERNAL (NON-NASA) USERS

A letter for Non-NASA users which transmits the applicable NASA policies must be provided to all non-NASA users while using the SED MPP IT Science Systems, or when using NASA systems and applications in general. These responsibilities must also be included in the training about security points of contact, and included in interagency agreements or other formal agreements or documents between NASA and other organizations.

6.0 ACKNOWLEDGEMENT

I acknowledge receipt of these Rules of Behavior, I understand my responsibilities, and I will comply with the Rules of Behavior for the NASA SED MPP IT Science Systems.

Name of User (Print)

Signature of User

Date